

## Re: local admin account password

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-11/0157.html>

---

**From:** Peterson Ellis ([peter\\_ellis\\_at\\_bah.com](mailto:peter_ellis_at_bah.com))

**Date:** 11/26/03

Date: Wed, 26 Nov 2003 13:08:00 -0500

To: dave kleiman <[dave@isecureu.com](mailto:dave@isecureu.com)>

I like Dave's suggestion, but I don't think that it goes far enough.

What I think would be a better scheme is to set a very complex\* random password when the box is first configured. The person doing the configuration would use that password to complete the job and then just leave it in place. The password would not be re-used on any other computers. When work that requires the local administrator password needs done, the tech uses a password reset disk to access the system.

Why I think this make the most sense:

1. The local administrator password, which is typically very weak, is replaced with a very strong one.
2. Eliminates the single point of attack that the proposed database scheme presents.
3. Does not affect most administrative duties that are normally performed by the domain admin.
4. Simpler for service people because they just need to remember a reset disk or where to download one from the web.
5. This eliminates the vulnerability created by weak admin passwords without replacing it with other vulnerabilities or un-needed complexity.

Ellis

\* 15+ characters mixed upper, lower, and special.

dave kleiman wrote:

>

> *1. Do you think if someone wanted to break the local admin account they could just boot to Password recovery disk and change the password?*

>

> *If you make them all the same you are thinking if one get compromised they all get compromised. So you make them all different. How about a standard*

SecurityFocus Microsoft: Re: local admin account password

> password with the last 5 digits of the MAC of that box in between. Thinking  
> that is still too easy then I would say you are dealing with someone who  
> would just use the idea I listed in number 1.

>

> You could mask the passwords with little tricks, or make the local admins  
> (unusable) but it sounds like a lot of work.

>

> Try checking: <http://www.securityfocus.com/archive/88/312263>

>

>

>

> \_\_\_\_\_  
> Dave Kleiman, CISSP, MCSE, CIFI

> dave@isecureu.com

> www.SecurityBreachResponse.com

>

> "High achievement always takes place in the framework of high expectation."

> Jack Kinder

>

>

>

> -----Original Message-----

> From: Eli Allen [mailto:ellen@bcpl.net]

> Sent: Tuesday, November 25, 2003 13:47

> To: focus-ms@securityfocus.com

> Subject: local admin account password

>

> Say you have more than 1000 systems, how do you handle the local admin  
> account password on the machines? (assuming it needs to be available for  
> extreme cases to get into the machine as you'd normally just use a domain  
> login)

>

> A few ways I can think of (in order from what I think is worst to best):

> 1) use the same password on all boxes. Obviously insecure

>

> 2) Use a different password on all boxes and a big filing cabinet to secure  
> it (as its impossible to memorize). Don't think this would work in the real  
> world so not worth using.

>

> 3) Use a password scheme where the password is basically the same on all box  
> except its based on something specific about the server. This means if  
> someone figures out the scheme (cracking a single box and figuring it out or  
> just gets told) they basically made this as good as the first idea I list.

>

> 4) Only use domain accounts so delete the local ones. But this means no  
> more recovery console and don't think cached logins will work. With so many  
> boxes and hence lots of admins you may not have logged onto the box and so  
> not have cached login in the cache even if you increased the logins that can  
> be cached.

>

> 5) My main idea/plan is to store all the passwords on a central SQL server.

> This way you can easily have a different random passwords for the admin

Re: local admin account password

SecurityFocus Microsoft: Re: local admin account password

- > *accounts on all the boxes.*
- >
- > *The DB file would be encrypted with EFS so only the limited user SQL runs*
- > *under has access to the file and another user just used for doing backups of*
- > *this file. This means an attacker can't use an OS break-in to get to the*
- > *data and needs to compromise SQL or one of those two user accounts. SQL*
- > *would be set to integrated auth and only allow the domain groups who are*
- > *allowed access to the admin password in. (i.e. using the access rights*
- > *already existing)*
- >
- > *For data recovery (this DB is very important not to lose) there are two main*
- > *considerations, one the file is small as the DB has very little info in it*
- > *and two it doesn't get updated very often. The backup user can make a zip*
- > *backup of the DB whenever it gets changed and then encrypt the file (PGP or*
- > *something like it with the private key stored on a/multiple CD-R(s)*
- > *somewhere safe) Then this file could be copied to lots of employee's*
- > *desktops. Its encrypted so they can't read it and with lots of people*
- > *having the file the likelihood of everyone's copy being damaged from HDD*
- > *failure is low. (Yes will use tape backup of the file too including off site*
- > *storage but tape is slow and should only be used if necessary) If there is*
- > *an emergency the managers could easily allow the file to be decrypted and*
- > *then attached to any SQL server available relatively quickly.*
- >
- > *Access to this file can be made by any utility that can make use of stored*
- > *procedures. There would be basically two stored procs, one to get a*
- > *password from the DB and one to set the password in the DB both would have 3*
- > *values (machine name, username, and password) passed in and out (obviously*
- > *depending on which you use). This way if a person decides to try and dump*
- > *the DB and get all the passwords the stored proc can do something about it*
- > *(alert management, stop it from happening, or something like that) This way*
- > *its easy to write whatever interface you want to be able to do access the DB*
- > *and the app itself doesn't really need to be secure as the authentication is*
- > *based on the user that app is run by.*
- >
- > *Yes I realize it has a central point of attack at the DB but I think that*
- > *can be secured well enough and the design is secure that its still better*
- > *then the other methods.*
- >
- > *Any comments? Thanks*
- >
- > *Eli Allen*
- > *eallen@bcpl.net*
- >
- >
- 
- >
- 
- >
- >
- 
- >

SecurityFocus Microsoft: Re: local admin account password

-----  
-----  
-----